UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/913,884	03/08/2002	Jean-Sebastien Coron	032326-161	5848

21839 7590 07/19/2007
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER	
HENNING, MATTHEW T	
ART UNIT	PAPER NUMBER
2131	
MAIL DATE	DELIVERY MODE
07/19/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/913,884	CORON ET AL.	
	Examiner	Art Unit	
	Matthew T. Henning	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 May 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *24-37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *24-37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *29 March 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

This action is in response to the communication filed on 5/8/2007.

DETAILED ACTION

Response to Arguments

Applicant's arguments with respect to claims 24-37 have been considered and are not found persuasive.

The applicant has requested a more detailed explanation of where Kocher2 teaches the following limitations:

A) What is being interpreted as the first random number?

B) What is being interpreted as the second random number?

C) Where is the first random number permuted?

D) Where is the second random number permuted?

E) Where is the XOR of the results of these permuted random numbers?

Regarding A), the first random number of Kocher2 is comprised of the bits 'b' (random blinding bits) as disclosed in Col. 12 Lines 45-47 and shown in pseudo-code in Col. 11 Lines 57-63 (the section labeled "Blind: temp=blinded input, dataOut=unblinding factor").

Regarding B), the second random number of Kocher2 is comprised of the bits of TEMP, which is disclosed as being the result of XOR operation between the input and the random blinding bits, as can be seen in Col. 12 Lines 47-50, as well as being shown in pseudo-code in Col. 11 Lines 57-63 (the section labeled "Blind: temp=blinded input, dataOut=unblinding factor"). Note that in the pseudo-code, a '^' represents the XOR operation.

Regarding C), the first random number is permuted when the output buffer is initialized with the blinding bits, as seen in Col. 12 Lines 51-53, as well as being shown in pseudo-code in Col. 11 Lines 57-63 (the section labeled "Blind: temp=blinded input, dataOut=unblinding factor"). This becomes clearer upon examining the pseudo-code of Kocher2, and upon understanding that "table[p]" is the permutation table (See Kocher2 Col. 11 Lines 20-21), wherein each of the 64 random blinding bits (first random number) is placed in the output buffer "dataOut" according to the permutation table "table[p]". This occurs in the pseudo-code "dataOut[table[p]]=b;".

The following example may be helpful in understanding how permutation is occurring according to Kocher2. For simplicity sake, the following example assumes 4 bit permutation instead of the 64 bit permutation used in the example pseudo-code of Kocher2. The example further assumes that perm[i]=i. This assumption is being made because perm[i] is simply used to change the time at which each bit is permuted, so that, for example, bit 2 is permuted first as opposed to bit 0 being permuted first. Perm[i] is irrelevant to the explanation of where the permutation occurs, and by assuming that perm[i]=i, p=i and we can just replace all the 'p's with 'i's in the pseudo-code.

Example:

table[i] = [2, 1, 3, 0] (that is table[0]=2, table[1]=1, table[2]=3, and table[3]=0)

b[i] = [a, b, c, d] (letters are being used to help illustrate the permutation)

dataOut[table[i]] = b[i]

So when i = 0, table[i] = table[0] = 2, so dataOut[2] is filled with the first random blinding bit b[0], which is a.

When i = 1, table[i] = table[1] = 1, so dataOut[1] is filled with the second random blinding bit b[1], which is b.

When i = 2, table[i] = table[2] = 3, so dataOut[3] is filled with the first random blinding bit b[2], which is c.

When i = 3, table[i] = table[3] = 0, so the fourth bit of dataOut is filled with the first random blinding bit b[3], which is d.

This results in dataOut[] containing the permuted random blinding bits [d, b, a, c].

As can be seen from the above example, the first random number has been permuted and stored in dataOut[].

Regarding D), the second random number (temp[]) is permuted when Kocher2 performs the final bit permutation, as seen in Col. 12 Lines 1-10 and 56-59. Similar to the explanation of C) above, the permutation of the blinded input temp[] occurs in the step:

dataOut[table[p]] ^ = temp[p] (in the pseudo-code "^" is XOR)

This step permutes the data in temp[p] to the location indicated by table[p], XOR's temp[p] with the permuted first random number stored at dataOut[table[p]], and stores the result of this XOR in dataOut[table[p]].

Regarding E), the permuted first random number is XORed with the permuted second random number when Kocher2 performs the final bit permutation, as seen in Col. 12 Lines 1-10 and 56-60. Similar to the explanation of C) above, the permutation of the second random number temp[] occurs in the step:

dataOut[table[p]] ^ = temp[p] (in the pseudo-code "^" is XOR)

This step permutes the second random number in temp[p] to the location indicated by table[p], XOR's temp[p] with the permuted first random number stored at dataOut[table[p]], and stores the result of this XOR in dataOut[table[p]].

The examiner has shown how Kocher2 does, in fact, teach the claim limitations which have been contested by the applicant, and, as such, has maintained the previously presented prior art rejections.

Claims 1-23 have been cancelled and claims 24-37 have been examined.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 24-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher et al. (US Patent Number 6,278,783) hereinafter referred to as Kocher1, and further in view of Kocher et al. (US Patent Number 6,327,661) hereinafter referred to as Kocher2.

Regarding claim 24, Kocher1 disclosed a countermeasure method in an electronic component that implements the DES cryptographic algorithm in which multiple rounds of calculation are performed on input data (See Kocher1 Abstract), wherein each round of calculation includes at least the following operations: a first permutation of data (See Kocher1

Col. 10 Lines 55-60); manipulation of the permuted data by a secret key (See Kocher1 Col. 10 Line 61 – Col. 11 Line 5); a table look-up operation based on the manipulated data (See Kocher1 Col. 11 Lines 6-7); and a second permutation of data (See Kocher1 Col. 11 Lines 7-11), but Kocher1 failed to disclose wherein, for a plurality of successive rounds of said algorithm, at least one of said first and second permutations of data comprises the following steps: selecting a first random value having the same size as the data being permuted, performing an exclusive-or operation between the data being permuted and the first random value to generate a second random value, executing said permutation operation on each of the first and second random values, to generate respective first and second random results, and performing an exclusive-or operation between said first and second random results to produce a final permuted result.

Kocher2 teaches that in order to protect against external monitoring attacks, processes, including DES permutations, should be performed using a leak-minimized permutation operation (See Kocher2 Col. 10 Line 50 – Col. 13 Line 19). Kocher further describes that the permutation operations should be altered by selecting a first random value having the same size as the data being permuted, performing an exclusive-or operation between the data being permuted and the first random value to generate a second random value, executing said permutation operation on each of the first and second random values, to generate respective first and second random results, and performing an exclusive-or operation between said first and second random results to produce a final permuted result (See Kocher Col. 12 Lines 20-60).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Kocher2 in the DES system of Kocher1 by performing the permutation processing according to the leak-minimized permutation operation. This would

have been obvious because the ordinary person skilled in the art would have been motivated to protect the permutation processing from external monitoring attacks.

Regarding claim 31, Kocher1 disclosed an electronic component that implements the DES cryptographic algorithm in which multiple rounds of calculation are performed on input data, said electronic component including a microprocessor that executes the following operations during each round of calculation (See Kocher1 Abstract): a first permutation of data (See Kocher1 Col. 10 Lines 55-60); manipulation of the permuted data by a secret key (See Kocher1 Col. 10 Line 61 – Col. 11 Line 5); a table look-up operation based on the manipulated data (See Kocher1 Col. 11 Lines 6-7); and a second permutation of data (See Kocher1 Col. 11 Lines 7-11), but Kocher1 failed to disclose wherein, for a plurality of successive rounds of said algorithm, at least one of said first and second permutations of data comprises the following steps: selecting a first random value having the same size as the data being permuted, performing an exclusive-or operation between the data being permuted and the first random value to generate a second random value, executing said permutation operation on each of the first and second random values, to generate respective first and second random results, and performing an exclusive-or operation between said first and second random results to produce a final permuted result.

Kocher2 teaches that in order to protect against external monitoring attacks, processes, including DES permutations, should be performed using a leak-minimized permutation operation (See Kocher2 Col. 10 Line 50 – Col. 13 Line 19). Kocher further describes that the permutation operations should be altered by selecting a first random value having the same size as the data being permuted, performing an exclusive-or operation between the data being permuted and the

first random value to generate a second random value, executing said permutation operation on each of the first and second random values, to generate respective first and second random results, and performing an exclusive-or operation between said first and second random results to produce a final permuted result (See Kocher Col. 12 Lines 20-60).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Kocher2 in the DES system of Kocher1 by performing the permutation processing according to the leak-minimized permutation operation. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect the permutation processing from external monitoring attacks.

Regarding claims 25 and 32, Kocher1 and Kocher2 disclosed performing both of said first and second permutation operations in each of said plurality of successive rounds (See the rejection of claims 24 and 31 above).

Regarding claims 26 and 33, Kocher1 and Kocher2 disclosed that the first and second permutation operations utilize different respective first random values (See Kocher2 Col. 12 Lines 45-47).

Regarding claims 27 and 34, Kocher1 and Kocher2 disclosed that said plurality of successive rounds comprise a first set of successive rounds consisting of the first three rounds of said algorithm, and a second set of successive rounds consisting of the last three rounds of said algorithm (See the rejection of claims 24 and 31 above as well as Kocher1 Fig. 1).

Regarding claims 28 and 35, Kocher1 and Kocher2 disclosed that the manipulation operation performed during said plurality of successive rounds comprises the following steps: performing an exclusive-or operation between said secret key and a third random value having

the same size as said key, to generate a fourth random value; performing bit-by-bit operations on each of said third and fourth random values to produce a pair of intermediate keys; manipulating the result of said first permutation operation with one of said intermediate keys to produce an intermediate result, and manipulating said intermediate result with the other of said intermediate keys to produce an output data item (See Kocher1 Col. 10 Lines 16-24 and the rejections of claims 24 and 31 above).

Regarding claims 29 and 36, Kocher1 and Kocher2 disclosed that said manipulating steps comprise exclusive-or operations (See Kocher2 Col. 12 Lines 45-50).

Regarding claims 30 and 37, Kocher1 and Kocher2 disclosed that said bit-by-bit operations comprise a key permutation operation, a shift operation and a compression permutation operation (See Kocher1 Col. 10 Lines 16-24).

Conclusion

Claims 1-23 have been cancelled and claims 24-37 have been rejected.

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Matthew Henning
Assistant Examiner
Art Unit 2131
7/12/2007

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100